Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs

SAMUEL LEE*

To start a business in an information-driven economy, a business must prepare itself to gather and store its clients and customers' personal information—social security numbers, driver's license numbers, account numbers—so it can provide efficient, narrowly tailored services and gain or maintain a winning advantage in an increasingly crowded domestic and international marketplace. As information is continually being gathered and retained, consumer concern regarding identity theft and overall personal privacy amplifies, and this concern has become a catalyst for the creation of numerous consumer protection laws, federal privacy laws, state privacy laws, and now, breach notification laws. The states have responded with a myriad of state laws with different notification triggers and different standards of notification, and the federal government is prepared to establish a federal breach notification standard of its own. This note will examine current state breach notification laws and a number of proposed federal breach notification bills, and assess how the laws affect a business' compliance strategy.

I. INTRODUCTION

To start a business in an information-driven economy, a start-up must prepare itself to gather and store its clients and customers' personal information—Social Security numbers, driver's license numbers, account numbers—so it can provide efficient, narrowly tailored services and gain a winning advantage in an increasingly crowded domestic and international marketplace. An array of businesses and organizations gather and store customers' sensitive, personal information for business use and data warehousing. Financial institutions and insurance companies gather the most private of financial information when customers open accounts and purchase various insurance policies. Educational institutions keep lengthy personal records of thousands of students, faculty, and employees. Grocery

* J.D., The Ohio State University Moritz College of Law, expected 2007. I'd like to thank Kirk Herath for all his help and guidance.

stores create databases tracking consumer shopping habits that are instantly retrievable with the swipe of a keychain bonus card. As information is continually being gathered and retained, consumer concern regarding identity theft[1] and overall personal privacy heightens. The concern has become a catalyst for the creation of numerous consumer protection laws, federal and state privacy laws, and now, state breach notification laws.

Businesses within the banking and insurance industries and other large businesses have already responded to security breaches, consumer backlash, and current governmental regulation by implementing technological safeguards and servicing customers' complaints. But what do startup businesses need to do to comply? How do these breach notification laws affect their bottom-line? Compliance has been a way of life for many corporate governance boards and small business owners, and for entrepreneurs to ensure their business practices comply with state and federal privacy laws they should integrate compliance strategies into their initial business plans, instead of waiting until a problem arises. Startups need to be appraised of the law, consider their business, and then decide what needs to be done to ensure legal compliance and financial success.

This Note will examine current state breach notification laws and a number of proposed federal breach notification bills and assess how the laws affect a business' compliance strategy. Section II will go into detail about recent history of high profile security breaches. Section III will discuss the various state laws that currently exist and examine their similarities and differences. Section IV will analyze competing federal bills and discuss a potential federal law's effect on businesses. Finally, Section V will discuss how start-up businesses can begin to think about complying with these laws, while preserving their entrepreneurial ambitions.

---

[1] In 2005, the Federal Trade Commission (FTC) advised the Senate Commerce Committee that its 2003 survey revealed that 10 million consumers were victims of identity theft, which lead to business losses of $48 billion and countless hours remedying consumer records. *Data Security Breaches—What You Need to Know Now, Goodwin Procter LLP*, MONDAQ BUSINESS BRIEFING, Oct. 4, 2005, at 14, *available at* http://www.mondaq.com/article.asp?articleid=35220. In 2004, approximately thirty-nine percent of fraud complaints to the FTC were related to identity theft, which was an increase of nineteen percent over 2003 and sixty-one percent over 2002. Zach Patton, *Stolen Identities*, GOVERNING MAG., Aug. 2005, at 39, *available at* http://www.governing.com/articles/8ident.htm. When a company's records are breached, the breach does not necessarily lead to identity theft or even present consumers with an immediate threat to their privacy, but consumer trust is rattled. According to a survey sponsored by the Ponemon Institute, a privacy think-tank, nineteen percent of Americans notified of a security breach are planning to terminate or have terminated their relationship with the affected company. Robert L. Raskopf and David Bender, *New Survey, Litigation Highlight Importance of Privacy Practices*, 234 N.Y. L.J. 63, Sept. 29, 2005, at 5 *available at* http://www.whitecase.com/publications/detail.aspx?publication=23. Another forty percent are considering switching companies, and another fifty-eight percent said their trust and confidence in the company has decreased. *Id.*

II. HISTORY AND CURRENT CLIMATE

Breach notification laws are not the first laws to attempt to regulate data protection and breach notifications. The Health Information Portability and Accountability Act gave the Department of Health and Human Services the ability to regulate the use and dissemination of information related to health care and "health plans, health care clearinghouses, and certain health care providers."[2] The Gramm-Leach-Bliley Act ("GLBA"), in existence since 1999, was designed to promote and enforce safeguarding[3] guidelines and data privacy standards in the institutional financial sector, which includes a set of customer notification requirements for financial or insurance companies governed by federal law.[4] The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice mandates that customer notification under GLBA occur when there is an unauthorized access of sensitive customer information and there is a likelihood that the information will be misused.[5] GLBA and analogous state privacy laws do not cover all businesses, but state breach notification laws have expanded these kinds of notification requirements to a broader and more general range of agencies and businesses. The media attention around many high-profile data breaches did not start the privacy and notification conversation, but it did help raise consciousness of the rising concern involving data safeguarding and data privacy. A look into some of the more high-profile breaches and various responses by state and federal agencies provides the context for the rush of breach notification bills and laws enacted in 2005.

A. *Security Breaches*

High profile security breaches at companies like ChoicePoint, Bank of America, LexisNexis,[6] University of California,[7] and Designer Shoe

---

[2] James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 10-11 (2005).

[3] For the purposes of this Note there is a distinction between data safeguarding and data privacy. Safeguarding refers to issues of protection and security of personal data. Privacy rules dictate the collection, dissemination, notification, and other uses of personal data.

[4] *See* Edward J. Janger & Paul M. Schwartz, *Modern Studies in Privacy Law: Notice, Autonomy and Enforcement of Data Privacy Legislation: The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1224 (2002).

[5] Federal Reserve Board, *Interagency Guidelines Establishing Information Security Standards Small-Entity Compliance Guide*, 11 (2005), *available at* http://www.federalreserve.gov/BoardDocs/Press/bcreg/2005/20051214/attachment.pdf.

[6] LexisNexis notified 32,000 persons on March 10, 2005, that their sensitive personal information was exposed. The Privacy Rights Clearinghouse, *A Chronology of Data Breaches Reported Since the ChoicePoint Incident*, http://www.privacyrights.org/ar/

Warehouse ("DSW") occurred in 2004 and 2005, the most notorious being the high-profile security breach at ChoicePoint. In February 2005, ChoicePoint, a data management broker based in Alpharetta, Georgia, publicly notified approximately 145,000 customers that thieves posing as potential small business customers had compromised their personal information in September 2004.[8] By November 2005, ChoicePoint had notified an additional 17,000 customers of breaches.[9] As of July 2005, ChoicePoint had spent $11.4 million remedying the security breach and it is expected that they will sacrifice $15 to $20 million in sales to overhaul their business to prevent future breaches.[10]

Shortly after the ChoicePoint announcement, Bank of America, one of the nation's largest banks, reported it had lost backup tapes that contained information of 1.2 million accounts that consisted of Social Security numbers and account information.[11] In April 2005, online broker Ameritrade disclosed that it had also lost backup tapes and notified 200,000 past and current customers of its loss.[12]

In June 2005, CardSystems, a transaction processing company that does business with credit card companies including Visa and Mastercard, announced that almost 40 million customer accounts were exposed during a breach.[13] The effects of this breach reached all the way to Japan, where a reported $1 million of fraudulent charges were made that were directly linked to the security breach earlier that month at CardSystems.[14]

As of February 2006, the Privacy Rights Clearinghouse, a consumer advocacy group in San Diego, has reported that since the ChoicePoint announcement almost 55 million customer accounts, containing sensitive information, spanning at least 80 different occurrences in a plethora of organizations, have been compromised. Most of those

---

ChronDataBreaches.htm (last visited Feb. 28, 2006).

[7] The University of California notified 98,400 persons on March 11, 2005, that their sensitive personal information was exposed. The Privacy Rights Clearinghouse, *supra* note 6.

[8] Associated Press, *17,000 More Warned in ChoicePoint Breach*, Nov. 9, 2005, http://www.msnbc.msn.com/id/9978812/from/RL.1/ (last visited Feb. 15, 2006).

[9] *Id.*

[10] Joris Evers, *Break-in Costs ChoicePoint Millions*, CNET News.com, July 20, 2005, http://news.com.com/Break-in+costs+ChoicePoint+millions/2100-7350_3-5797213.html (last visited Feb. 15, 2006).

[11] Associated Press, *Bank of America Loses Customer Data*, Mar. 1, 2005, http://www.msnbc.msn.com/id/7032779/.

[12] Bob Sullivan, *Ameritrade Warns 200,000 Clients of Lost Data*, April 19, 2005, http://www.msnbc.msn.com/id/7561268/ (last visited Feb.15, 2006).

[13] Steven Marlin, *Banks Scramble To Contain Damage From CardSystems Hacking Incident*, INFORMATIONWEEK, June 22, 2005, http://informationweek.com/story/showArticle.jhtml?articleID=164901831 (last visited Feb. 15, 2006).

[14] Peralte C. Paul, *Fraud in Japan Tied to Data Breach; Atlanta-based Card Process Blamed*, THE ATLANTA JOURNAL-CONSTITUTION, June 23, 2005, at 1E.

breaches were linked to dishonest insiders, computer hacking, or stolen laptops and computers.[15]

B. *State and Federal Agency Response*

State and federal agencies imposed civil fines on businesses for lax data security long before breach notification laws existed.[16] Enforcement has come from the Federal Trade Commission ("FTC") under the Federal Trade Commission Act or states' attorneys general under unfair and deceptive trade practices statutes.[17] In June 2005, BJ's Wholesale Club agreed to settle charges by the FTC related to its failure to maintain appropriate security measures to protect sensitive personal information of its customers.[18] Using the Federal Trade Commission Act, the FTC claimed that BJ's lax security led to unauthorized access of customer information, which led to "millions of dollars of fraudulent purchases."[19] The settlement required an overhaul of BJ's information security program and third party auditing every other year for twenty years.[20]

In April 2004, New York State Attorney General Eliot Spitzer announced an agreement with BarnesandNoble.com to correct an Internet security breach and a flaw in its system that led to an exposure of customers' personal information.[21] The agreement required a security program, employee training, external auditing, compliance reports, and a $60,000 fine.[22]

In Ohio, Attorney General Jim Petro brought suit against local retailer Designer Shoe Warehouse ("DSW") demanding that it individually notify each customer whose private information was exposed due to stolen computer files.[23] The stolen data included DSW "customers' names, credit card numbers, debit card numbers, checking account numbers, and driver's license numbers."[24]

---

[15] *See* Privacy Rights Clearinghouse, *supra* note 6.

[16] Most of the charges revolved around state and federal security and privacy laws, not breach notification laws.

[17] *See* Press Release, Federal Trade Commission, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.htm (last visited Feb. 15, 2006); Press Release, Off. of N.Y. St. Att'y Gen. Off. Eliot Spitzer, Attorney General Reaches Agreement with Barnes and Noble on Privacy and Security Standards (Apr. 29, 2004), *available at* http://www.oag.state.ny.us/press/2004/apr/apr29a_04.html (last visited Feb. 15, 2006).

[18] *See* Press Release, Federal Trade Commission, *supra* note 17.

[19] *Id.*

[20] *Id.*

[21] Press Release, Off. of N.Y. St. Att'y Gen. Off. Eliot Spitzer, *supra* note 17.

[22] *Id.*

[23] *Ohio Sues DSW Over Customer Data Theft*, Consumeraffairs.com, June 7, 2005, http://www.consumeraffairs.com/news04/2005/ohio_dsw.html (last visited Feb. 15, 2006).

[24] *Id.*

In early 2006, the FTC imposed a $10 million civil fine on ChoicePoint for its security breach, and an additional $5 million settlement that will be used to create a trust fund to help the victims of the data theft.[25] The charge was based on ChoicePoint's failure to comply with data protection requirements promulgated by the Fair Credit Reporting Act and that ChoicePoint had made false and misleading statements regarding its data privacy policies.[26]

In February 2006, CardSystems and its successor Solidus Networks, Inc., doing business as Pay By Touch Solutions, agreed to settle FTC charges.[27] The settlement will require CardSystems and Pay By Touch to implement a comprehensive security program and obtain auditing every other year for twenty years.[28] The CardSystems breach lead to the exposure of tens of millions of customers' personal information.[29]

State attorneys general and the FTC have been using data privacy laws to attack companies that do not safely protect individuals' personal information, but now, state legislatures have responded to these security breaches by passing or introducing breach notification laws that require companies to disclose breaches that meet the state requirements for disclosure.

III. STATE BREACH NOTIFICATION LAWS

As of January 2006, at least twenty-three states[30] have introduced or passed breach notification laws, affecting companies who do business in those states.[31] Most state laws mirror California's law, with some even adopting California's statutory language verbatim. Others have diverged from the pivotal predecessor by adding and subtracting language; thus, narrowing or broadening the ambit of the law's ability to require an

---

[25] Jaikumar Vijayan, *FTC Makes a Point With ChoicePoint Penalties; Hits Firm with Largest Civil Fine Ever in Data Breach Case*, COMPUTERWORLD, Jan. 30, 2006, http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,108173,00.html?source=x52 (last visited Feb. 15, 2006).

[26] *Id.*

[27] Press Release, Federal Trade Commission, CardSystems Solutions Settles FTC Charges (Feb. 23, 2006), *available at* http://www.ftc.gov/opa/2006/02/cardsystems_r.htm (last visited Mar. 1, 2006).

[28] *Id.*

[29] *Id.*

[30] As of January 2006, the following states have passed breach notification laws: Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, and Washington. The State PIRG, *State PIRG Summary of State Security Freeze and Security Breach Notification Laws*, http://www.pirg.org/consumer/credit/statelaws.htm (last visited Feb. 14, 2006).

[31] *Id.*

organization to notify affected customers. To determine how breach notification laws affect a business, most state laws can be evaluated by four characteristics: (1) what are the "triggers" to notification, (2) what is the appropriate mode and method of notification, (3) is notification to outside regulators and agencies required, and (4) what safe harbors exist. These general categories will dictate much of the costs involved with compliance and provide a template by which each state law can be evaluated and compared. California's breach notification law has been the most influential, and many states have followed its example. It is important to discuss its merits first to provide a frame of reference to view the other state laws, and later to view proposed federal bills. After a discussion of California's law, a sample of other effectuated state laws will display the variations of current breach notification laws.

A. *California (SB 1386)*

Many state notification laws resemble California's Senate Bill 1386. Enacted in 2003, the passage of SB 1386 came after another high-profile security breach[32] at the Stephen P. Teale Data Center.[33] The breach led to the exposure of the personal information of 265,000 state employees, including 120 legislators, and the two month notification delay infuriated many senators and assembly members.[34] With a unanimous vote, the bill passed and entered the national scene when ChoicePoint, a Georgia corporation, and other companies responded to the California law and publicly notified customers of security breaches.

The purpose behind SB 1386 was to limit the effects of privacy and financial security breaches created by the "widespread collection of personal information by both the public and private sector."[35] Specifically, the Act is designed to fight the growing crime of identity theft and other crimes using personal information as source material.[36] The language of the law reads:

> Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been,

---

[32] It is mildly ironic that such a significant breach that prompted the creation of such a law occurred at a state agency and not a corporation.

[33] Deb Kollars, *U.S. Follows State's Lead on Data-Theft Notification*, SACRAMENTO BEE, June 22, 2005, at A1.

[34] *Id.*

[35] S.B. 1386, *Chapter 915*, 2001-02 Reg. Sess. (Cal. 2002).

[36] *Id.*

> acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay...."[37]

The "trigger" based on the statutory language in California law is comprised of several different elements that combine to create a minimum threshold to notification. Once the different requirements of the trigger are met, then a company or organization is required to notify affected individuals. The first element California requires is an actual occurrence or *reasonable belief* that an unauthorized acquisition has occurred.[38] This reasonable belief standard is broad, and requires notification after any security breach, but the California privacy office narrows the definition of "acquisition" to mean physical possession and control of personal information, downloading, or possession of information used in some illegal manner such as opening fraudulent accounts or executing identify theft.[39] While California's privacy office's definition is not law, it is persuasive. California further limits the kind of information the law protects to personal information that is computerized.[40]

Protected "personal information" is defined as an "individual's first name or first initial and last name in combination with . . . [a] Social Security number, driver's license number or California identification card number, or account number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account."[41] The law notes that a breach has not occurred if an employee or agent accesses personal information within their scope of employment or agency as long as good faith requirements are met and no additional unauthorized information is disclosed.[42]

California law allows for a variety of methods of notification. "Notice" may be provided as written notice, electronic notice, and if relevant, substitute notice which includes email notice, conspicuous posting of the notice on the agency's web site page, or notification to major statewide media.[43] Substitute notification is permitted when the cost of notification exceeds $250,000, there are 500,000 affected individuals, or the person does not have enough contact information to provide written or

---

[37] CAL. CIVIL CODE § 1798.29(a) (Deering 2005).
[38] *Id.*
[39] Office of Privacy Protection, *Recommended Practices on Notification of Security Breach Involving Personal Information*, http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf (last visited Feb. 15, 2006).
[40] § 1798.29(a).
[41] CAL. CIVIL CODE § 1798.29(e) (Deering 2005).
[42] CAL. CIVIL CODE § 1798.29(d) (Deering 2005).
[43] CAL. CIVIL CODE § 1798.29(g) (Deering 2005).

electronic notice.[44] Notification needs to be expedient, and should be done within ten days of the breach.[45]

One significant safe harbor exists under SB 1386. California law has provided that notification is not required if personal information is encrypted. Therefore, organizations that encrypt their personal information do not fall under the breach notification requirement.[46]

California's trigger elements are one of the broadest state triggers to notification. Essentially, California requires a company or organization to notify customers whenever there is a reasonable belief a breach has occurred. The more narrowed definition of acquisition constrains the law's scope, but the law is still broader than those of other states that have chosen to require notification only after some kind of risk of harm assessment.

California's law has been pivotal and because many companies do business with California residents, most companies have made steps to overhaul their security programs and notification methods to comply with California law. California's SB 1386 is by no means perfectly constructed and various attempts have been made to amend the law to remove some of the exemptions the statute has created.[47] As debate rages on whether a national federal standard should exist, other states have responded in similar and dissimilar ways to California.

B. *Other State Notification Laws*

In 2005, at least 35 states have enacted or introduced their own version of breach notification laws.[48] Most states follow the California template, but some states like Arkansas, Delaware, and New York have created laws with different notification trigger levels, notification methods and specificity requirements, outside reporting requirements, and safe harbors.

1. Arkansas (SB 1167)

Under Arkansas law, before notification is required there must be a reasonable belief that an unauthorized person has acquired computerized, unencrypted personal information.[49] This is almost identical to California's standard. But, unlike California law, Arkansas law provides that

---

[44] CAL. CIVIL CODE § 1798.29(g)(3) (Deering 2005).
[45] Office of Privacy Protection, *supra* note 39.
[46] CAL. CIVIL CODE § 1798.29(a) (Deering 2005).
[47] *See* Thomas Claburn, *Law Requires ChoicePoint To Disclose Fraud*, INFORMATIONWEEK, Feb. 17, 2005, http://www.informationweek.com/showArticle.jhtml?articleID=60401882 (last visited Feb. 15, 2006) (stating that Senator Debra Bowen attempted to amend California law to extend to all forms of data, not just computerized, but was voted down).
[48] The State PIRG, *supra* note 31.
[49] ARK. CODE ANN. § 4-110-105(a) (Lexis 2005).

"notification under this section is *not* required if, after a reasonable investigation, the person or business determines that there is no *reasonable likelihood of harm* to customers."[50] This exemption does not exist in California law. This exemption creates a narrower trigger to notification than California's trigger. A business is not required to notify Arkansas residents of security breaches if the business can prove there is no reasonable likelihood that harm will result. Under California law, most breaches, even those that may not reasonably lead to harm to the customer, need to be reported to the public. Arkansas also expanded its definition of "personal information" to include a person's name in combination with medical information.[51]

2. Delaware (HB 116)

Delaware, like Arkansas, has narrowed its notification trigger,[52] but unlike Arkansas, Delaware requires businesses and individuals to "conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused."[53] Notice is required once an investigation shows that information has been or is reasonably likely to be misused.[54] Yet Delaware has gone one step further than Arkansas. Arkansas allows businesses and organizations to investigate a security breach and assess the reasonableness of resulting harm to its customers if it does not want to notify.[55] Because Delaware did not include its investigation requirement as an exemption to notification, a company appears to be required to do a good faith investigation.[56] Mandatory investigations incur additional costs and businesses that want to opt-out of a belaboring investigation no longer have this option.

Delaware also differs from most other states by not including the word "encryption" in its statutory language. This exclusion is significant, because the potential safe harbor created by states like California with the encryption language does not exist in Delaware.

Delaware expands its permitted notification methods to allow telephonic notification. Substitute notification is permitted if notice costs exceed $75,000; there are more than 100,000 affected customers; or the individual does not have enough contact information to provide written, telephonic, or electronic notice.[57]

---

[50] ARK. CODE ANN. § 4-110-105(d) (Lexis 2005) (emphasis added).
[51] ARK. CODE ANN. § 4-110-103 (7)(D) (Lexis 2005).
[52] *See* DEL. CODE ANN. tit. 6, § 12B-102(a) (Lexis 2005).
[53] *Id.*
[54] *Id.*
[55] *See* ARK. CODE ANN. § 4-110-105(d) (Lexis 2005).
[56] *See* DEL. CODE ANN. tit. 6, § 12B-102(a) (Lexis 2005).
[57] DEL. CODE ANN. tit. 6, §12B-101(3) (Lexis 2005).

Delaware does not have a private right of action, but allows the state attorney general to bring actions for violations of the statute.[58]

3. New York (AB 4254/SB 5827)

New York's notification law is virtually identical to California's law, but it goes further and adds specificity where California's law does not. California law does not codify its definition of acquisition, but leaves its meaning to the office of privacy as a recommended best practice. Some factors New York says a business may consider in determining whether information has been acquired by an unauthorized person include physical possession and control, such as a stolen computer or device; downloading or copying; or unauthorized usage of the information, such as the opening of fraudulent accounts or identify theft.[59]

New York asks for more detail in a company disclosed notification than California. A notification under New York law should have the contact information for the person making the notification and list the categories of information that were affected, including elements of information that have been or are reasonably believed to have been acquired.[60]

New York law, unlike most state laws, has codified outside reporting requirements when a breach has occurred. If 5,000 New York residents are notified at a single time, New York law requires additional notification to consumer reporting agencies of the timing, content, and distribution of the notices and approximate number of affected persons.[61] Also, when a business or person is required to notify a resident, they must give notice to the state attorney general, the consumer protection board, and the state Office of Cyber Security and Critical Infrastructure Coordination of the timing, distribution, and content of the notice and the approximate number of affected individuals.[62]

States have responded to concerns over identity theft and protection of personal information by enacting breach notification laws, which require businesses and organizations to notify customers in the event their personal information is acquired by an unauthorized person. Most states have mirrored California's influential law, but there are competing state statutes that differ from California's standards. States like Delaware have created laws that, on their surface, call for less notification than California. Other states like New York make the notification process expensive and laborious by requiring outside reporting along with regular notification. California's law still stands as the most influential, but as the idea of a uniform federal

---

[58] DEL. CODE ANN. tit. 6, §12B-104 (Lexis 2005).
[59] N.Y. GEN. BUS. LAW § 899-aa(1)(c) (McKinney 2005).
[60] N.Y. GEN. BUS. LAW § 899-aa(7) (McKinney 2005).
[61] N.Y. GEN. BUS. LAW § 899-aa(8)(b) (McKinney 2005).
[62] N.Y. GEN. BUS. LAW § 899-aa(8)(a) (McKinney 2005).

law to govern breach notifications comes closer to realization, it will be a compelling question as to which state law, if any, the federal law will attempt to emulate.

IV. FEDERAL RESPONSE

At the close of 2005, there were at least seven[63] House and Senate committees working on federal legislation directly addressing what organizations should do when individuals' personal and private data has been illegally accessed.[64] The likelihood of federal legislation has increased now that at least twenty-three state legislatures have passed their own versions of breach notification laws, creating a patchwork of conflicting laws that burden interstate commerce.[65] Most of the federal bills mirror or build off of some variation of existing state law, but the operative question remains: "Which concepts will Congress adopt?"

Various federal bills have been in the works for most of 2005, but because of divergent opinions regarding committee jurisdiction, statutory language, and scope of the potential law, a consensus has not been reached.[66] The potential ramifications of a uniform federal law have many groups and organizations contributing their opinions to the process. The opinions of diverse players—corporations, consumer advocacy groups, government organizations, government representatives, and state governments—circle around many different issues, but the main issue is the trigger language. This section will look at the trigger language and construction of Senate Bill 1789, House Bill 3140, and Senate Bill 1326.[67] After an analysis of those bills, the section will transition into a brief look at the varying opinions of industry and consumer groups about a federal bill and their recommendations for its potential construction.

---

[63] S.1789 109th Cong. (2005); S.1408, 109th Cong. (2005); S.1326, 109th Cong. (2005); H.R. 4127, 109th Cong. (2005); S. 500, 109th Cong. (2005); H.R. 1080, 109th Cong. (2005); H.R. 3997, 109th Cong. (2005); H.R 3140, 109th Cong. (2005).

[64] *See* Florence Olsen, *Debate Continues on Data Privacy Bill*, FEDERAL COMPUTER WEEK, Nov. 21, 2005, http://www.fcw.com/article91504-11-21-05-Print (last visited Feb. 15, 2006).

[65] The State PIRG, *supra* note 31.

[66] *See* Olsen, *supra* note 64.

[67] Any of these bills could change before final enactment, but the purpose of looking through the various federal bills is to provide a general idea of what form a uniform federal law may take and to illuminate the different effects statutory language will have on organizations.

A. *Proposed Federal Laws*

1. S. 1789

Various bills have been presented in both houses of Congress, but Senate Bill 1789, the Personal Data Privacy and Security Act of 2005, is one of the most complex bills.[68] Its contents have been amended and scrutinized on various occasions since its introduction on September 29, 2005, by Republican Senator Arlen Specter of Pennsylvania and Democratic Senator Patrick Leahy of Vermont,[69] but the Senate Judiciary Committee eventually passed it on November 17, 2005.[70] Senate Bill 1789 requires individual customer notification as follows:

> Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information shall, following the discovery of a security breach of such information notify any resident of United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.[71]

A significant safe harbor exception exists in this bill that directly defines the scope of the bill's proposed trigger. The general trigger is a reasonable belief that sensitive personally identifiable information has been accessed or acquired.[72] The exception to this general rule is that no notification is required if a risk assessment concludes that there is no significant risk that the security breach has resulted in, or will result in, harm to the individual.[73] After the discovery of the breach, an agency or business must notify the Secret Service[74] of the results of the risk assessment and its decision to invoke the risk assessment exemption.[75] For the exemption to be final, the Secret Service must not indicate, in writing,

---

[68] Alexei Alexis, *Senate Judiciary Committee Passes Chairman's Comprehensive ID Theft Bill*, 4 PRIVACY & SECURITY L. REP. 1420 (Nov. 21, 2005), *available at* http://pubs.bna.com/ip/BNA/PVL.NSF/85256269004a991e8525611300214487/7d02526b6e20dd84852570bd0080134a?OpenDocument (last visited Feb. 15, 2006).

[69] S. 1789, 109th Cong. (2005).

[70] *Id.*

[71] S. 1789, 109th Cong. § 321(a) (2005).

[72] *Id.*

[73] S. 1789, 109th Cong. § 322 (b)(1) (2005).

[74] The Secret Service does not seem to be the prime enforcing agency to perform risk assessments, but the enforcement agencies are mostly linked to the specific committee presenting the bill.

[75] S. 1789, 109th Cong. § 322 (b)(2)(A)-(B) (2005).

that notice should be given.[76] With this risk assessment exemption, the real trigger in S. 1789 is the *significant risk of harm* standard, which then leads to the subsequent notification of the proper regulatory agency.[77]

"Sensitive personally identifiable information" has been defined as any information in electronic or digital form that includes an individual's first and last name or first initial and last name in combination with any one of the following data elements: non-truncated Social Security number, driver's license number, passport number, or alien registration number,[78] or any two of the following: home address or telephone number, mother's maiden name (if identified as such), or date of birth.[79] Other data elements include unique biometric data such as fingerprints or retina images, unique codes,[80] identification numbers with password or access code required to obtain money or other things of value,[81] and financial account numbers in combination with passwords and access codes.[82]

Notification can occur in a variety of methods. The bill permits written notice, telephone notice, or email notice if the individual has consented to receive such electronic notice.[83] Media notice is acceptable where 5,000 persons in a given state or jurisdiction have had their sensitive personally identifiable information accessed.[84] The bill requires certain content requirements, such as a description of categories of information that has been accessed, toll-free numbers of the business entity, and numbers of credit reporting agencies.[85]

Senate Bill 1789 goes further in setting specifications for notifying other entities after a breach of sensitive personally identifiable information. The bill requires an agency or business to notify, without unreasonable delay, all consumer reporting agencies if more than one thousand individuals' information has been compromised.[86] The United States Secret Service will be the source of federal enforcement and investigation,[87] and notification to the United States Secret Service shall be required if any one of four situations occur: (1) the number of individuals affected exceeds 10,000; (2) the security breach involves a database or system of databases containing the sensitive personally identifiable information of more than 1,000,000 individuals nationwide; (3) the security breach involves databases owned by the federal government; or (4) the security breach

---

[76] S. 1789, 109th Cong. § 322(b)(3) (2005).
[77] *See* S. 1789, 109th Cong. § 322 (2005).
[78] S. 1789, 109th Cong. § 3(11)(A)(i)(2005).
[79] S. 1789, 109th Cong. § 3(11)(A)(ii)(2005).
[80] S. 1789, 109th Cong. § 3(11)(A)(iii)(2005).
[81] S. 1789, 109th Cong. § 3(11)(A)(iv)(2005).
[82] S. 1789, 109th Cong. § 3(11)(B) (2005).
[83] S. 1789, 109th Cong. § 323(1)(2005).
[84] S. 1789, 109th Cong. § 323(2) (2005).
[85] *See* S. 1789, 109th Cong. § 324 (2005).
[86] S. 1789, 109th Cong. § 325 (2005).
[87] S. 1789, 109th Cong. § 1039(c) (2005).

involves primarily sensitive personally identifiable information of employees and contractors of the federal government involved in national security or law enforcement.[88] Senate Bill 1789 establishes general preemption of other federal and state laws except for the protocol required by the GLBA.[89]

The bill does, however, leave some content creation authority to the states. A state may add to content requirements by requiring notice to include information regarding victim protection assistance provided for by that state.[90] Also, in addition to state courts, a state attorney general has the ability to bring civil action in federal district court on the behalf of its residents.[91] The Act does not, however, create a private right of action.[92]

Additional provisions in the bill provide for requirements for a personal data privacy and security program,[93] a layout of civil remedies[94] and guidelines for the relationship between data brokers and individuals.[95] Another notable exemption exists where a business or agency will be exempted from notification requirements when they participate in a security program that is designed to block the use of the sensitive personally identifiable information before any charges on the individual's account can occur.[96]

Those who oppose or criticize the bill do so for a number of reasons. Information technology groups like the Business Software Alliance, the Information Technology Association of America ("ITAA"), and the Software & Information Industry Association claim that the "'no significant risk of harm' standard is 'confusing and cumbersome.'"[97] The information technology groups call for a more detailed standard that requires notification when there is significant risk of *identity theft*. Senator Sessions from Alabama was expected to introduce amendments to the bill that would change the notification standard to a "significant risk of identity

---

[88] S. 1789, 109th Cong. § 326(a) (2005).
[89] S. 1789, 109th Cong. § 329(a) (2005). The exemption essentially acknowledges that the GLBA already has extensive notification requirements and data safeguarding provisions.
[90] S. 1789, 109th Cong. § 324(b) (2005).
[91] S. 1789, 109th Cong. § 328(a)(1) (2005).
[92] S. 1789, 109th Cong. § 328(f) (2005).
[93] *See* S. 1789, 109th Cong. § 302 (2005).
[94] *See* S. 1789, 109th Cong. §§ 327, 328.
[95] *See* S. 1789, 109th Cong. § 301 (2005).
[96] *See* S. 1789, 109th Cong. § 322(c)(1)(A) (2005).
[97] Alexei Alexis & Rachel McTague, *Specter-Leahy ID Theft Measure Would Harm Industry, Groups Say*, 4 PRIVACY & SECURITY L. REP. 1294 (Oct. 24, 2005), *available at* http://pubs.bna.com/ip/BNA/PVL.NSF/85256269004a991e8525611300214487/1c83993d340ede07852570a200000e66?OpenDocument (last visited Feb. 15, 2006).

theft" standard instead of "significant risk of harm" standard.[98] This amendment never materialized.[99] Sessions also stated that he worried that Specter's bill would preserve a patchwork of state laws instead of creating a strong uniform national standard.[100] The Financial Services Coordinating Council, an organization consisting of associations representing the banking, securities, and insurance industries, also voiced concern that the bill may not be a strong uniform law. The council, in a letter to Congress in October 2005, stated the legislation "would put in place a duplicative and inconsistent system of federal and state regulation and enforcement that could have far-reaching and negative consequences for the financial services system and our customers."[101] Senator Leahy, a cosponsor of the bill, voiced concerns over the bill's broad preemption[102] and Senator Feinstein, at one point, pushed to have health care data protected under the bill but relented.[103]

2. H.R. 3140

By the end of 2005, a number of Senate and House bills were in the markup stage or being reviewed by judiciary committees. An example of a bill originating in the House is H.R. 3140.

Democratic Representative Melissa Bean of Illinois introduced H.R. 3140, the Consumer Data Security and Notification Act of 2005, on June 30, 2005.[104] The pertinent trigger language reads:

> The regulations prescribed under subsection (b) shall include requirements for the notification of consumers following the discovery of a breach of security of any data system maintained by the consumer reporting agency in which sensitive consumer information was, or is reasonably believed to have been, acquired by an unauthorized person.[105]

---

[98] Alexei Alexis, *Senate Judiciary Republicans Seek More Time on Chairman's ID Theft Bill*, 4 PRIVACY & SECURITY L. REP. 1356 (Nov. 7, 2005), *available at* http://pubs.bna.com/ip/BNA/PVL.NSF/85256269004a991e8525611300214487/ff9091626b843810852570af00829896?OpenDocument (last visited Mar. 13, 2006).

[99] *Id.*

[100] Alexis, *supra* note 68.

[101] Alexis, *supra* note 97.

[102] Alexei Alexis, *Senate Judiciary Begins Work on Chairman's ID Theft Measure*, 4 PRIVACY & SECURITY L. REP. 1328 (Oct. 31, 2005), http://pubs.bna.com/ip/BNA/PVL.NSF/4866a14be3b6f56685256ba3004dcb8b/c180be6c0dea54e0852570a8007b7f79?OpenDocument (last visited Feb. 15, 2006).

[103] Alexis, *supra* note 98.

[104] H.R. 3140, 109th Cong. (2005).

[105] H.R. 3140, 109th Cong. § 630(c)(1) (2005).

Notification is not required where an agency reasonably concludes that misuse of the information is unlikely to occur,[106] notifies the appropriate law enforcement agency,[107] and takes appropriate steps to remedy the situation and safeguard the individual's interests.[108] Specter's standard of "risk of significant harm" seems more narrow than the "unlikely misuse" standard in H.R. 3140, but how much narrower is unclear. H.R. 3140 provides another level of exemption where the data that is compromised is encrypted.[109] If the personal data is encrypted then an agency is permitted to reasonably conclude misuse is unlikely to occur.[110] It is not stated whether state attorneys general will be permitted to file actions on behalf of their citizens, or if the regulatory enforcement agency will be the sole entity allowed to bring civil suits.[111]

3. S. 1326

Introduced on June 28, 2005, by Republican Jeff Sessions,[112] Senate Bill 1326 takes a different stance on the development of a federal notification standard compared to Specter's bill. The pertinent notification language reads:

> If an agency or person that owns or licenses computerized data containing sensitive personal information, determines, after discovery and reasonable investigation . . . that a significant risk of identity theft exists as a result of a breach of security of the system of such agency or person containing such data, the agency or person shall notify any individual whose sensitive personal information was compromised if such individual is known to be a resident of the United States.[113]

Senator Session's bill calls for notification when there is a significant risk of identity theft, which is much narrower language than S. 1789's significant risk of harm language. "Identity theft" is defined as "fraud committed using the identification of another person with the intent to commit, or to aid or abet any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or

---

[106] H.R. 3140, 109th Cong. § 630(c)(2)(A)(i) (2005).
[107] H.R. 3140, 109th Cong. § 630(c)(2)(A)(ii) (2005).
[108] H.R. 3140, 109th Cong. § 630(c)(2)(A)(iii) (2005).
[109] *See* H.R 3140, 109th Cong. § 630(c)(3)(A) (2005).
[110] *Id.*
[111] *See* H.R. 3140, 109th Cong. (2005).
[112] S. 1326, 109th Cong. (2005).
[113] S. 1326, 109th Cong. § 3(b)(1)(A) (2005).

local law and that results in economic loss to the individual."[114] It is unclear, however, how much more narrow of a standard S. 1326's language presents. While S. 1326's definition of identity theft is directly affiliated with fraud and unlawful activity, S. 1789's notification standard of significant risk of harm standard, until paired down or later defined by the United States Secret Service, seems to encompass more than just fraud and unlawful activity. In practice, the narrower identity theft language of S. 1326 would allow agencies or businesses to notify fewer individuals than required by Senator Specter's bill.[115]

Additional notification requirements are conspicuously absent in this version of Senator Session's bill.[116] Senate Bill 1789 required notification to the enforcing body, the United States Secret Service, after the intention of using that bill's significant harm exemption, but S. 1326 does not possess such a notification requirement and only goes as far as requiring a notification to consumer reporting agencies when 1,000 or more individuals need to be notified.[117]

Senate Bill 1326 is a less complex bill than its Senate counterpart, S. 1789, and its preemption section does not stray from that trend. Blanket preemption of state law would occur under S. 1326,[118] and once the department of justice files an action, a state attorney general may not bring an action for any violation of the Act alleged in the complaint.[119]

B. *Industry and Consumer Response to Federal Bills*

The mishmash of state law and federal bills has not gone unnoticed by industry and consumer groups that have scrutinized the state laws and federal bills at every junction of their evolution. Groups generally fall into one of three categories of thought: a federal bill is unnecessary because state law is adequate, a broad federal law which completely preempts state law is favored, or a more narrow federal law is needed that preempts stronger state law, but eliminates redundancy and over-notification.

The first tier of debate revolves around the very existence of a uniform federal law. Edmund Mierzwinski, program director at the US Public Interest Research Group ("PIRG"), made clear in his testimony

---

[114] S. 1326, 109th Cong. § 2(6) (2005).

[115] An organization may not have to notify as many affected individuals, but best business practices will likely compel businesses to go beyond what the law provides as a minimum notification threshold. This does not nullify the entire debate over trigger language because the *significant risk of harm* language may be so vague that it requires notification when a business would deem it necessary or beneficial to notify customers. *Compare* S. 1326, 109th Cong. § 3(b)(1)(A) (2005), *with* S. 1789, 109th Cong. (2005).

[116] *See* S. 1326, 109 Cong. (2005).

[117] S. 1326, 109th Cong. § 3(b)(6) (2005).

[118] S. 1326, 109th Cong. § 5 (2005).

[119] S. 1326, 109th Cong. § 4(a)(2)(D)(i) (2005).

before a committee in Congress that many consumer group organizations feel that state responses have been adequate, and they fear a federal response could further restrain state responses.[120] Consumer groups feel that disregarding states' efforts would be detrimental to consumers because it ignores the valuable input and laboratorial study that states provide in the process of creating public policy.[121] The PIRG points out that even before the numerous state laws, attorneys general forced compliance under California law, which essentially served as a de-facto standard.[122] California law provides for notification when there is a *reasonable belief an unauthorized acquisition* has occurred.[123] Many states have fashioned their trigger language after California's reasonable belief standard, which prompts notification with simple acquisition and does not ask for the additional significant risk factors which Senator Specter's bill and Session's bill require. Those bills seemingly narrow the instances when an agency or business will be required to notify individuals, but California's reasonable belief standard may not regulate non-California agencies or businesses choosing a piecemeal notification strategy, complying with the bare minimum of each individual state law. This approach would be unwise but is hypothetically viable if the status quo is upheld.

Those who favor a uniform federal law to govern notification, like Ira Hammerman, Senior Vice President and General Counsel of the Securities Industry Association, believe the "expanding patchwork of state – and local – laws affecting data security and notice will make effective compliance very difficult for us and equally confusing for consumers."[124] Kirk Herath, Chief Privacy Officer at Nationwide Mutual Insurance Co., favors a federal uniform standard because, besides the various state triggers, notification content requirements differ from state to state and not all states provide safe harbor provisions exempting companies that encrypt data.[125] He also finds a central regulatory authority enforcing a single law a much better alternative than state attorneys general enforcing their own state laws because it is difficult to operate in interstate commerce with a patchwork

---

[120] *Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft Before the Committee on Banking, Housing and Urban Affairs*, 109th Cong. 2 (2005), *available at* http://banking.senate.gov/_files/ACFDC9B.pdf (statement of Edmund Mierzwinski, U.S. PIRG).

[121] *Id.*

[122] *See id.*

[123] CAL. CIVIL CODE § 1798.29(a) (Deering 2005).

[124] *Examining the Financial Service Industry's Responsibility to Prevent Identity Theft and Protect Sensitive Consumer Financial Information Before the Committee on Banking, Housing and Urban Affairs*, 109th Cong. 1 (2005), *available at* http://banking.senate.gov/_files/hammerman.pdf (statement of Ira Hammerman, Securities Industry Association).

[125] Jaikumar Vijayan, *Three More States Add Laws on Data Breaches*, COMPUTERWORLD, Jan. 6, 2006, http://www.computerworld.com/databasetopics/data/story/0,10801,107530,00.html (last visited Feb. 15, 2006).

quilt of conflicting laws.[126] Microsoft Senior Vice President and General Counsel, Brad Smith, also favors federal legislation and sees an enactment of a comprehensive federal law as one step closer to a harmonization of the U.S. and international privacy approaches.[127] Smith advised that commerce is growing increasingly global, and Microsoft and other multi-national companies want to provide a safe level of privacy and data protection to international customers.[128]

A federal bill is likely to pass regardless of consumer group opposition, so the battle moves to the actual construction of the future federal law. Public interest groups like PIRG have recommended that if a federal law was to be enacted, it should cover computerized and paper data, disallow encryption exemptions, provide for free credit reports, and notification should be triggered by unauthorized acquisition rather than reasonable or significant risk of harm or identify theft.[129] This option would essentially enact the California standard as the official federal standard and call for a broad trigger to notification. Currently, no federal bill has such a broad trigger.[130] Senator Specter's original bill, S. 1332, which was introduced in June 2005, proposed that notification be required after any breach that "impacts sensitive personally identifiable information."[131] This standard did not survive, and S. 1332 was eventually replaced by S. 1789, which narrowed the notification trigger by adding the *significant risk of harm* language. A letter to Congress by more than 40 state attorneys general stated that a federal bill should not preempt state law or ignore California's *de facto* standard, but as a compromise, the significant risk of harm language would be acceptable if additional notification to law enforcement was required.[132]

Whether a broad trigger takes the form of California's "reasonable belief of acquisition" standard or Senator Specter's "significant risk of harm" standard, consumer groups are pushing for a sufficiently broad trigger to ensure prompt notification to individuals who have had their most

---

[126] *Id.*

[127] Microsoft PressPass for Journalists, *Microsoft Addresses Need for Comprehensive Federal Data Privacy Legislation*, http://www.microsoft.com/presspass/features/2005/nov05/11-03Privacy.mspx (last visited Feb. 15, 2006).

[128] *Id.*

[129] Mierzwinski, *supra* note 120, at 8-10.

[130] Specter's bill's trigger language is broader than a *risk of identity theft*, but appears to be more vague than broad when compared to California's law. California's law has defined its trigger language, but it is still uncertain what exactly Specter's *significant risk of harm* standard actually encompasses.

[131] S. 1332, 109th Cong. § 421(a) (2005).

[132] Alexei Alexis, *State AGs Urge Congress to Establish Broad Data Breach Notification Standards*, 4 PRIVACY & SECURITY L. REP. 1357 (Nov. 7, 2005) *available at* http://pubs.bna.com/ip/BNA/PVL.NSF/85256269004a991e8525611300214487/ab8a6d28cfd12309852570af00829898?OpenDocument (last visited Feb. 15, 2006).

sensitive personal information compromised. Consumer groups in favor of a broad trigger and stringent reporting requirements, coupled with strong and uniform enforcement, believe a weak federal bill with a narrow trigger would be unable to help individuals combat identity theft and other fraud pertaining to compromised personal information.[133] They dislike trigger language that narrows notification to occurrences where there is a reasonable belief of a significant risk of identity theft because they believe the standard would allow companies to notify only certain select individuals, leaving others at risk.[134] In a letter to House committees, four significant consumer privacy groups[135] voiced concern that a trigger—specifically H.R. 4127's standard—tied to a risk of identity theft standard would not be effective because identity thieves wait a few months before striking.[136] Therefore, immediate evaluation of risk of identity theft after a security breach may not be feasible.[137] Consumer groups also raise concerns that identity theft is not the only crime or harm that can be perpetuated with personal information—stalking and domestic violence being examples that fall outside reporting requirements—but if identity theft is not reasonably foreseen, then no notification will occur.[138]

Not everyone opposes a narrow bill, and many see a broad bill as cumbersome. Representative Cliff Stearns voiced a fear that "a broader notification standard would drive up costs for businesses and inundate consumers with meaningless warnings".[139] The Security Industry Association stated that a broad trigger like California's standard leads to over-notification, and companies will run the risk of unnecessarily confusing and frightening consumers, and, possibly, desensitizing or numbing consumers to future notifications.[140] The ITAA provides that a more narrow federal law based on the risk of identity theft clearly articulates when notification is required and will help companies distinguish between security breaches that pose legitimate threats and those that do not.[141]

---

[133] *See* Letter from US PIRG, Privacy Right Clearinghouse, Electronic Privacy Rights Center, and Consumers Union to Subcommittee on Commerce, Trade, and Consumer Protection and Committee on Energy and Commerce (Nov. 2, 2005), *available at* http://www.uspirg.org/consumer/archives/4127ltrfinal.pdf (last visited Feb. 15, 2006).
[134] *See id.*
[135] US PIRG, Privacy Right Clearinghouse, Electronic Privacy Rights Center, and Consumers Union.
[136] Letter, *supra* note 133.
[137] Letter, *supra* note 133.
[138] *Id.*
[139] Grant Gross, *Data Breach Bills Unlikely to Pass Before 2006*, INFOWORLD, Nov. 21, 2005, http://www.infoworld.com/article/05/11/11/HNdatabreachbill_1.html (last visited Apr. 6, 2006).
[140] Hammerman, *supra* note 124, at 8-9.
[141] Alexis, *supra* note 102.

At this point, the makeup of a federal law is uncertain. Congress has and will continue to maneuver trigger language, additional notification requirements, content requirements, and preemption policies to strike a balance, but regardless of what Congress does, businesses, especially smaller startup businesses, should be prepared to comply with the final federal product or current state laws.

V. BUSINESS ISSUES FOR ENTREPRENEURS TO CONSIDER

When entrepreneurs start businesses, they should be looking at more than just executing brilliant business plans, aggressive marketing, and sound financial planning; they also need to be developing cost-effective data safeguarding and privacy compliance schemes. The temptation to overlook the importance of legal compliance always exists, but in the case of breach notification laws, data safeguarding requirements, and other privacy laws, an oversight can lead to even more disastrous effects to small startup business that have little room for customer dissatisfaction and defection. Because identity theft has for six years been the number one consumer complaint to the Federal Trade Commission,[142] it is not economical for any business to ignore issues of data security or breach notification. Knowing this reality, a startup business needs to react to breach notification and data safeguard laws with great care and deference, but the costs associated with compliance can be expensive and timely. A balance can occur, and new business ventures should look to larger corporations for examples on how to protect data and assist customers. Implementing procedures that large corporations have adopted may be too costly, so an efficient process needs to be created. Even though the status and structure of a uniform federal law is unknown, a business can still make the proper steps to position itself for absolute compliance and more importantly, customer satisfaction. Notification is a result of misfortune or failure, so it is appropriate to begin with ideas of how startup businesses can protect themselves. But once they are protected they must also determine what the best course of action is when something does go wrong and the law requires them to notify individuals of a breach.

---

[142] *See* Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data*, 5 (Jan. 25, 2006), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (last visited Feb. 15, 2006).

A. *Data Security*[143]

Financial services companies have created security programs to comply with data safeguarding provisions of federal laws like GLBA,[144] and other corporations have been keen to bolster their security programs to avoid actions from state attorneys general and the FTC under unfair and deceptive trade practices statutes.[145] Data security ideas exist, and companies like Microsoft, Inc. have suggested a few practical ways to prepare for a security breach.[146] They stress encryption, development of a disaster plan, storage of only absolutely necessary information, and discontinuing the use of Social Security numbers.[147] Oracle, Inc., in response to California's standards, suggested similar tips for compliance, and they added some additional ways to bolster one's data security program. Businesses should not store credit card numbers in their entirety, implement security related training programs for employees, make use of cryptographic hashes, manage user authorization centrally, and make use of other advanced technological safeguards.[148] These suggestions may look simple and appealing to startup businesses, but one must assess their effectiveness in a smaller business environment, specifically the effectiveness of encryption, the discontinued use of personal information, and the use of GLBA standards as a template for compliance.

1. Encryption

California's SB 1386 provides businesses a safe harbor: one does not have to notify individuals if the private information accessed is encrypted.[149] It is unknown whether a federal law will have an encryption safe harbor, but as Microsoft suggests, encryption is a strong way to protect data. According to Eric Ouellet, Vice President of Research and Privacy at Gartner in Connecticut, many companies have already started to model their

---

[143] Up to this point, most of the discussion has been about breach notification laws. A slight divergence into data security is necessary to continue the breach notification discussion because businesses are better off not having to avoid any individual under any law by protecting their duty and implementing sound business practices to ensure security.

[144] *See* Janger, *supra* note 4.

[145] *See* Press Release, Federal Trade Commission, *supra* note 17; Press Release, *See also* Off. of N.Y. St. Att'y Gen. Off. Eliot Spitzer, *supra* note 17.

[146] *See* Mircosoft Technet, *Legal Briefs: Breach Notification Laws*, http://www.microsoft.com/technet/technetmag/issues/2006/01/LegalBriefs/default.aspx (last visited Feb. 15, 2006).

[147] *Id.*

[148] Oracle Product Stack, Best Practices for California SB 1386, http://www.oracle.com/technology/deploy/security/db_security/pdf/oracle_sb_1386.pdf (last visited Feb. 15, 2006).

[149] CAL. CIVIL CODE § 1798.29(a) (Deering 2005).

own best practices in the spirit of breach notification laws, and this includes embracing encryption and other protective schemes.[150] Unfortunately, high-end encryption technology is costly[151] and there is a debate over which applications and technologies are the most effective.[152] The encryption process is not only potentially expensive, high end encryption can be complex and lengthy,[153] and unless a business plans to encrypt data once and let it sit idle, a business will have to go through the process of accurately decrypting, re-encrypting, and storing the data for future use.[154] A number of other drawbacks exist with the encryption technology: potential slowed performance of computer systems, difficulty managing keys to encrypt and decrypt data, insiders still have access to keys, and increased difficulty managing and searching data once encrypted.[155] Encryption is a viable way to protect sensitive data, but a startup business should evaluate what options are most practical and relevant to its needs. Blanket encryption may be too costly and create unneeded complexity.[156] Technology is always changing, and the risk of technology becoming outdated or ineffective will always exist because each business is different, and the assessment of which data should be encrypted with which technology will need to be done on an ad hoc basis, considering protection, cost, and manageability.

2. Discontinue Use of Some Personal Information

The idea of storing and using the least amount of personal information possible is an economical approach and will help lower costs and minimize the amount of potentially exposed data. The idea of discontinuing the use of Social Security numbers is a logical suggestion, but if business practice involves accessing credit reports and other sensitive documents, it would be cumbersome, if not impossible, to use account numbers in place of Social Security numbers. Storing more information than what is needed to conduct business should be discouraged, but each business' requirements are different and it may be difficult to discontinue

---

[150] Lauren Bielski, *Operation Lockdown?,* ABA BANKING J., February 2006, at 62, *available at* http://www.allbusiness.com/periodicals/article/867452-1.html.

[151] Henry Baltazar, Secure Storage Tops Labs' New Year's Wish List, EWEEK.COM, Jan. 16, 2006, http://www.eweek.com/article2/0,1895,1909603,00.asp(last visited Feb. 15, 2006).

[152] Bielski, *supra* note 150.

[153] Baltazar, *supra* note 151.

[154] Interview with Kirk Herath, Chief Privacy Officer, Nationwide Mut. Ins. Co., in Columbus, OH. (Feb. 10, 2006).

[155] George V. Hulme, *Data Lockdown*, INFORMATIONWEEK, Apr. 19, 2004, http://www.informationweek.com/showArticle.jhtml?articleID=18901717 (last visited Feb. 15, 2006).

[156] Microsoft and Oracle suggest the use of encryption, but they are also the entities that sell encryption technology.

the gathering and storing of Social Security numbers, credit card numbers, and other sensitive information.

3. GLBA and Other Safeguarding Standards

Federal and state agencies have provided a plethora of best practice suggestions for businesses that need to comply with GLBA safeguarding standards and other state safeguarding regulation. For example, the Interagency Compliance Guidelines are a compilation of § 501(b) of the GLBA and § 216 of the Fair and Accurate Credit Transaction Act of 2003, and these guidelines were created to "establish standards relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and the proper disposal of customer information."[157] Benjamin Wright, a Dallas-based data security attorney, advises that the guidelines can be "a good reference for all businesses."[158] The guidelines recommend that a security program should be designed to suit the size and complexity of the business and the nature and scope of its activities.[159] Companies should identify reasonable internal and external threats to personal data, quantify the sensitivity of the data and ensure protection accordingly, continuously monitor computerized and paper information, ensure proper record disposal, train staff, and test key controls and computerized components.[160]

B. *Approaches to Notification*

Even if data is properly safeguarded, accidents happen.[161] Data security and employee protocol can do nothing to save a business' data when an employee loses a laptop, potentially exposing the sensitive personal information of thousands of customers. It would be unwise for a business, especially a new business with a smaller clientele, to hastily notify all customers if a breach occurs. A checklist created by Kirk J. Nahra provides for practical and helpful questions to think about after a security breach.[162] He suggests such questions as, "[D]o I have to notify anyone? If

---

[157] Federal Reserve Board, *supra* note 5, at 2-3.

[158] Donald G. Aplin, *Lawyer Says Recent GLB Guidance Is Good Reference for All Businesses*, 5 PRIVACY & SECURITY L. REP. 57 (Jan. 16, 2006), *available at* http://pubs.bna.com/ip/BNA/PVL.NSF/85256269004a991e8525611300214487/14c9a43250807e28852570f400831745?OpenDocument (last visited Feb. 15, 2006).

[159] Federal Reserve Board, *supra* note 5, at 5.

[160] *Id.* at 5-7, 12.

[161] Many of the data breaches in 2005 were not associated with data hackers, but with lost laptops and lost backup tapes. The Privacy Rights Clearinghouse, *supra* note 6.

[162] Kirk J. Nahra, *A 2006 Privacy and Security Compliance Checklist*, 5 PRIVACY & SECURITY L. REP. 144, (Jan. 30 2006), *available at* http://pubs.bna.com/ip/BNA/PVL.NSF/85256269004a991e8525611300214487/8d7dfeee2993b95385257104000802 72?OpenDocument (last visited Mar. 1, 2006).

so, whom must I notify and through what means? If I don't 'have to' notify, should I notify anyway? Is there anyone else I need to notify (clients, regulators, etc.)?"[163]

California's law essentially governs until another state provides a broader trigger or a federal law preempts state law, but even in the midst of uncertainty, businesses should take a general mind frame that if a security breach occurs, the business will do its personal best to "make things right." This "make things right" attitude could entail offering free one year credit monitoring, toll-free numbers for assistance, and other services to their customers when their personal information has been compromised.[164] It is in the business' best interest to minimize damages to avoid further lawsuits and complications. Most corporations have adopted these services as best practices[165] and it would be prudent for startup businesses to adopt similar practices.

The physical and financial cost of notification can be a significant burden to a business, but if done efficiently and professionally, notification can become an opportunity for businesses to distinguish themselves with their customer service. A business should review their notification content to make sure the message is clear and relevant, making sure the customer feels confident that the responsibility of monitoring and burden of clearing up any issues will fall on the business and not the customer. Multiple methods of notification should be deployed if deemed necessary to put customers on notice. Companies, of course, need not risk frightening consumers by flooding them with too much information. Also, over-notification could lead consumers to become desensitized to future occurrences.[166]

Businesses should inform individuals that identity theft is only one of many kinds of fraud people can commit with sensitive information. Individuals may not truly grasp the nuances of identity theft, and the realization that those who steal identities are looking for more than an opportunity to buy a few computers online but are hoping for long-term fraud.[167] Customers will appreciate the additional warning, and the warning may go as far as assisting in stopping future harm. There is a balance between frightening and servicing, and each business will need to make individual determinations along the way to find what is best for their business.

---

[163] *Id.*

[164] Interview with Kirk Herath, Chief Privacy Officer, Nationwide Mut. Ins. Co., in Columbus, OH. (Feb. 10, 2006).

[165] *Id.*

[166] *See* Hammerman, *supra* note 124, at 9.

[167] Interview with Kirk Herath, Chief Privacy Officer, Nationwide Mut. Ins. Co., in Columbus, OH. (Feb. 10, 2006).

VI. CONCLUSION

When entrepreneurs think about engaging in a new business venture, they may be tempted to craft their business plan and leave issues of privacy compliance as an afterthought. Entrepreneurs have limited ability to voice their opinions on how breach notification laws are managed or created, but if they did, they may ask for narrow notification triggers and limited reporting requirements—whatever balance allows for the most consumer protection at minimal cost. Breach notification laws should be clear so that business can be efficiently conducted, but consumer protection and confidence needs to be weighed. Triggers with a broad quantifying agent—whether it be "significant risk of harm", "misuse" or some derivation—will provide clarity for businesses but protect consumers from more than just identity theft. Reasonable reporting to credit reporting agencies and enforcement agencies should be required and civil actions should be limited to state attorneys general, but those who are planning a business do not have to wait for the law to settle. They can begin to investigate current data safeguarding and notification policies, but more importantly, they can begin to plan. If data safeguarding schemes and notification protocols can be addressed in the early formation stages of a business, then entrepreneurs will be able to save money and ward off future headaches.

Entrepreneurs should implement privacy and safeguarding compliance strategies into their business plans so they can comply with the law, but implementation of these legal issues does more than help businesses avoid fines and lawsuits. Implementation allows businesses to respect consumers' privacy expectations and create opportunities to be cost effective.